

# Payhembury Parish Council

## GDPR Data Breach Notification Policy

### Contents

1. Introduction .....	1
2. What is a personal data breach? .....	1
3. Consequences of a personal data breach .....	2
4. Data controller's duty to report a personal data breach to the ICO .....	2
5. Data controller's duty to notify an individual that a personal data breach has occurred.....	3
6. Data processor's duty to notify data controller of a personal data breach .....	4
7. Data breach awareness and designated responsibilities.....	4
8. Data controller's duty to record all personal data breaches .....	4

## 1. Introduction

- 1.1. Under the General Data Protection Regulation (GDPR) introduced on 25 May 2018, data controllers such as parish councils and parish meetings have an obligation to:
  - a. Keep an internal record of all personal data breaches
  - b. Report them within 72 hours to the ICO in certain circumstances
  - c. Notify an individual affected by a personal data breach in certain circumstances. Data processors also have an obligation to notify the data controller of a personal data breach without delay.
- 1.2. A personal data breach may have significant consequences for an individual whose data is affected. Personal data breaches may also cause reputational damage for the parish council responsible for the breach. In addition, failure to report a breach may result in intervention by the ICO which includes a fine up to £17.5 million or 4% of global turnover whichever is greater.
- 1.3. This document summarises the data breach reporting obligations and how Payhembury Parish Council will respond to a personal data breach should it occur.
- 1.4. This policy should be read in conjunction with the following Parish Council documents:
  - GDPR Data Protection Policy
  - GDPR Privacy Notice (General)
  - GDPR Privacy Notice (Staff, Councillors & role holders)
  - GDPR Subject Access Request (SAR) Procedure & GDPR SAR Form
  - Data Retention and Disposal Policy

## 2. What is a personal data breach?

- 2.1. GDPR defines this as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (Article 4 of GDPR). Examples of a personal data breach include:
  - access by an unauthorised third party;
  - deliberate or accidental action (or inaction) by a controller or processor;
  - sending personal data to an incorrect recipient;

# Payhembury Parish Council

## GDPR Data Breach Notification Policy

- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

2.2. Lawful handling of personal data includes taking steps to reduce the risk of the occurrence of personal data breaches. GDPR specifically requires data controllers and data processors to implement appropriate technical and organisational measures to ensure appropriate levels of security against the risks presented by processing personal data. The risks include the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data (Articles 5 and 32 of GDPR). The measures set out in GDPR include:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

### 3. Consequences of a personal data breach

3.1. Personal data is information held by a data controller or processor about an individual which identifies them and may, for example, include contact details, date of birth, bank details, information about their education, health, personal, business or working life or family. A breach of personal data may result in a loss of control over personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property, social disadvantage.

3.2. This means that a breach, depending on the circumstances in each case, can have a range of adverse effects on an individual, which include emotional distress, and physical and material damage.

### 4. Data controller's duty to report a personal data breach to the ICO

4.1. Payhembury Parish Council (The Data Controller) shall notify the ICO about a personal data breach if it is likely to result in 'a risk to the rights and freedoms' of an individual. The breach shall be reported 'without undue delay and, where feasible, not later than 72 hours after having become aware of it'. Where notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

4.2. Data breaches shall be notified to the ICO's website as follows - <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulationgdpr/personal-data-breaches/>

4.3. If a breach is likely to result in a risk to the rights and freedoms of an individual, notification shall:

- a. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- b. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

# Payhembury Parish Council

## GDPR Data Breach Notification Policy

- c. Describe the likely consequences of the personal data breach;
  - d. Describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 4.4. GDPR provides that in so far as it is not possible to provide the information above at the same time, the above information may be provided in phases without 'undue further delay'.

### 5. Data controller's duty to notify an individual that a personal data breach has occurred

- 5.1. If the personal data breach is likely to result in 'a high risk to the rights and freedoms' of an individual, this shall be communicated to the individual 'without undue delay'. This communication shall be in clear and plain language and include the nature of the personal data breach and the information set.
- 5.2. Examples of personal data breaches about which an affected individual would need to be notified are below:
- A ransomware attack which results in the parish council's electronic personal data being encrypted. Back-ups are not available and the data cannot be restored / made available to the parish council;
  - An HR file is left on a bus;
  - An ex-Clerk/Councillor refuses to return paper/electronic files containing personal data;
  - Unencrypted personal data is emailed to a Councillor's personal device and his emails are hacked;
  - A Councillor shares sensitive personal data about an individual via social media;
  - An old parish council computer which still contains personal data on the hard drive is donated to a local charity.
- 5.3. **Exemptions from mandate to notify an individual.**  
There are certain circumstances where there is no mandate to notify individuals. These include:
- where the data controller has implemented appropriate technical and organisational protection measures, and that those measures have rendered the personal data unintelligible to any person who is not authorised to access it, such as encryption;
  - where the data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of individual(s) is no longer likely to materialise or
  - where it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the individual(s) are informed in an equally effective manner.
- 5.4. Even when a data controller is excused from communicating with an individual for the reasons above, the GDPR provides that the ICO, who should already have been notified of the personal data breach, still has the power to require the data controller to inform the affected individual if it considers there is a high risk to the individual's rights and freedoms.

# Payhembury Parish Council

## GDPR Data Breach Notification Policy

### 6. Data processor's duty to notify data controller of a personal data breach

- 6.1. GDPR provides that when a data processor becomes aware of a personal data breach, it must notify the data controller of this 'without undue delay'.

### 7. Data breach awareness and designated responsibilities

- 7.1. Payhembury Parish Council shall ensure that awareness and training are provided to all members. At any time, anyone should be able recognise a data breach and raise / escalate the consideration of an incident to appropriate person(s) to:
  - a. determine whether a personal breach has occurred
  - b. respond appropriately.
- 7.2. The Clerk shall be responsible for reporting a data breach. The Clerk may consult with the Chairman, relevant Councillors and/or, as appropriate, with businesses which provide the Parish Council's IT support services and or host and maintain its server. A committee or sub-committee could not be responsible for investigating or responding to personal data breaches because the notice period for convening a meeting is inconsistent with the urgency of the work involved.

### 8. Data controller's duty to record all personal data breaches

- 8.1. Compliance against the statutory timescale GDPR requires a data controller to keep an internal record of all personal data breaches. This is regardless of whether or not they need to be reported to the ICO. Records shall comprise the facts relating to the personal data breach, its effects and the remedial action taken.
- 8.2. The Clerk shall establish and maintain appropriate records to satisfy the above requirements.